

SPECIFICATION

Electronic Version 1.2.8

Stylesheet Version 1.0

System and method for attaching un-forgeable biometric data to digital identity tokens and certificates, and validating the attached biometric data while validating digital identity tokens and certificates

Background of Invention

[0001] 1. Field of Invention.

[0002] This invention relates to the processes of issuing and validating digital certificates. More particularly, through the use of bound biometric data, the invention adds diligence and integrity to the process of issuing digital certificates and the process of validating digital certificates.

[0003] 2. Description of Terminology and Background Art.

[0004]

"Public key cryptography (PKC)" is a two key encryption and decryption process. The two keys together are referred to as an asymmetric key pair. With an asymmetric key system, each user has two keys: a public key and a private key. When one key is used for encryption, the other is used for decryption. With this technique, one key can be made publicly available, while the other key is kept secret with its owner or user. The keys are reflexive; that is: a) A message encrypted using a public key can be decrypted only by the owner/user of the matching private key, and b) conversely, a message encrypted with a private key can only be decrypted with the matching public

key. Example PKC algorithms, which comply with applicable government or commercial standards, are the digital signature algorithm (DSA/RSA) and secure hash algorithm (SHA-1/MD5).

[0005] Various aspects of public-key cryptographic (PKC) systems are described in the literature, including R. L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM vol. 21, pp. 120-126 (February 1978); M. E. Hellman, "The Mathematics of Public-Key Cryptography", Scientific American, vol. 234, no. 8, pp. 146-152, 154-157 (August 1979); and W. Diffie, "The First Ten Years of Public-Key Cryptography", Proceedings of the IEEE, vol. 76, pp. 560-577 (May 1988), "Communication Theory of Secrecy Systems", Bell Sys. Tech. J. vol. 28, pp. 656-715 (October 1949).

[0006] Refer to Figure 5 for a block diagram illustrating the process of using PKI to transmit an encrypted document over a public medium. In order to send an encrypted document to someone, you need a copy of their public key. You use their public key to encrypt the document, and they use their private key to decrypt the document.

[0007] Refer to Figure 6 for a block diagram illustrating the process of using PKI to digitally sign digital data. When a signer (a user) encrypts a document using a private key, and sends this encrypted document to other recipients (other users) who have access to the user's public key, these users can decrypt the document using the public key to access the original document. In a simple system, this can be visualized as a signer that has signed the document with his/her private key. The recipients can prove the identity of the signer because only the signer has the private key that matches the public key that recipients use for decryption. Practical PKI implementation is based on the fact that all signers sign documents using their private keys, while other users can verify the identity of the signers by using the signers' public keys.

[0008] Refer to Figure 7 for a block diagram illustrating the process of obtaining a digital certificate. Public and private keys are just numbers. To make digital certificates legally binding, there needs to be a mechanism in place to associate a public key to its owner (the user). A Certificate Authority (CA) performs this task. The user generates the two keys, and sends the public key and some personal information to a CA. The CA wraps up the information in a file, and then signs the file, thus creating a digital

certificate. When verifying a digital signature, a user looks at the signer's certificate and makes sure that the signature from the issuing CA is valid. To make legally binding signatures, a CA must go to great lengths to authenticate the certificate holder's identity. If an appropriate level of diligence is applied while issuing the certificate, such a certificate may reliably identify the owner of the public key pair, which is used to provide authentication, authorization, encryption, and non-repudiation services.

[0009] As illustrated in Figures 3a and 3b, a typical digital certificate has the following form: [Version, Serial No., Issuer Algorithm (Hash & Digital Signature), Issuer Distinguished Name (DN), Validity Period, Subject DN, Subject Public Key Info, Issuer Unique Identifier (optional), Subject Unique Identifier (optional), Issuer Public Key, Extensions (optional)]Issuer Digital Signature. A unique DN is formed by concatenating naming specific information (e.g., country, locality, organization, organization unit, e-mail address, common name).

[0010] Certificate extensions can be used as a way of associating additional attributes with users or public keys, and for managing the public key infrastructure certificate hierarchy. Guidance for using extensions is available in the recommendations of ITU X.509v3 (1993).verline. ISO/IEC 9594-8:1995, "The Directory: Authentication Framework" or in IETF Internet X.509 Public Key Infrastructure Certificate and CRL Profile <draft-ietf-pkix-ipki-part1-11>.

[0011] A user's digital certificate is often appended to an electronic document with the user's digital signature to facilitate the verification of the digital signature. Alternatively, the certificate may be retrieved from the issuing CA or directory archive.

[0012] The "Public Key Infrastructure (PKI)" is the hierarchy of CAs responsible for issuing digital certificates. Certificates and certification frameworks are described in C. R. Merrill, "Cryptography for Commerce--Beyond Clipper", The Data Law Report, vol. 2, no. 2, pp. 1, 4-11 (September 1994) and in the X.509 specification.

[0013] A "wrapper" is a digital structure that is used to contain digital data and optionally associated digital signatures in a standardized form. Examples of such standards are RSA PKCS #7, the W3C XML Signature Syntax and Processing Draft Recommendation,

S/MIME, PKIX, XHTML, and XFDL.

[0014] A "signature block" usually contains three components: signature data, certificate data, and metadata. Signature data contains the hash of the content encrypted with the private key of the signer, thus creating a digital signature. Certificate data contains the signer's digital certificate. The metadata contains details about the algorithms and methods used to create and define the signature and certificate.

[0015] 3. Description of the Problem[0001] Statistics show that more than one thousand cases of identity theft are reported in the United States alone each day. The single biggest enabling factor for fraud on the Internet is the anonymity inherent in many of the processes that occur there. Despite many attempts to resolve the situation, it remains trivial for anyone to impersonate another actual or fictitious person.

[0016] The best solution available for positive identification on the Internet is the service provided by certificate authorities. Digital certificate technology has been around for several years and is the means by which secure (SSL) transactions can be carried out on web sites. Certificate authorities issue digital certificates to both individuals and to web sites. Web sites with digital certificates are very common, less common is the use of digital certificates by people.

[0017] Although most people are not aware, many key products that they use already support digital certificates: MS Internet Explorer™, MS Outlook™, MS Outlook Express™, MS Windows Messenger™, Navigator™, and Lotus Notes™ are just a few examples. These products use digital certificates for identification, signing, and encryption. If you have a digital certificate, you may use it with one of these products to: identify yourself and others, sign documents and e-mails, and share encrypted data with colleagues.

[0018] A digital certificate is only as good as the diligence that was used to issue the certificate, and that is major limitation, because with very few exceptions, digital certificates are handed out to anyone with an e-mail address in any name he/she asks for. Some certificate authorities go an extra step and require the certificate applicant to answer some questions that appear on their credit report. This is not a viable solution due to the tremendous amount of identity theft and fraud that occurs in the

credit bureau industry.

Summary of Invention

- [0019] Presented here is a system and method that tie a person's true identity to that person's on-line activities.
- [0020] The system and method are equally suited to the task of issuing un-forgable digital ID cards on a smart card, much like an ATM card but with much more security. The system and method irrefutably bind a card holder's biometric data (photograph, fingerprints, voice print, etc.) to a digital certificate inside a smart card. This is a completely new twist on existing technology, and is easy to implement on existing computers and kiosks. A large benefit of this technology is that it provides absolutely positive identification in real time, without the need for a connection to a central database.
- [0021] The system and method facilitate positive identification in the physical world as well as on the Internet.

Brief Description of Drawings

- [0022] FIG. 1a is a highly abstracted block diagram of the data and processes involved in the standard certificate issuance process performed at a certificate authority.
- [0023] FIG. 1b is a highly abstracted block diagram of the data and processes involved in the modified (biometric data bound) certificate issuance process performed at a certificate authority.
- [0024] FIG. 2a is a highly abstracted block diagram of the data and processes involved in validating the authenticity of a digital certificate.
- [0025] FIG. 2b is a highly abstracted block diagram of the data and processes involved in validating the authenticity of a digital certificate; while simultaneously comparing the level of similarity between the biometric data derived from the certificate and biometric data supplied in from some other source.
- [0026] FIG. 3a is an abstracted block diagram of the data that comprises a standard X.509 certificate as defined by "CCITT, Recommendation X.509".

- [0027] FIG. 3b is an abstracted block diagram of the data that comprises a standard X.509 certificate with the addition of embedded biometric data; while maintaining full compliance with "CCITT, Recommendation X.509".
- [0028] FIG. 4a is an abstracted block diagram of the data that comprises a biometric data block with embedded biometric data.
- [0029] FIG. 4b is an abstracted block diagram of the data that comprises a biometric data block with referenced biometric data.
- [0030] FIG. 5a is an abstracted block diagram of the process of using PKC to encrypt data.
- [0031] FIG. 5b is an abstracted block diagram of the process of using PKC to decrypt data.
- [0032] FIG. 6a is an abstracted block diagram of the process of using PKC to digitally sign data.
- [0033] FIG. 6b is an abstracted block diagram of the process of using PKC to verify a digital signature.
- [0034] FIG. 7 is an abstracted block diagram of the process of using PKC and PKI to request, issue, and acquire a digital certificate.

Detailed Description

- [0035] The inventions can be implemented utilizing commercially available computer systems and technology to create and verify digital certificates with embedded biometric data.
- [0036] 1. Certificate Issuance.
- [0037] FIG. 1b is a block diagram of the data and process involved in the portion of the invention which embeds the biometrics into a digital certificate.
- [0038] In this process some form of biometric data is submitted to a certificate authority (CA) in such a manner as to positively associate the data with a digital certificate request. The methods for submitting the biometric data are not in the scope of the

invention.

[0039] Through currently established cryptographic procedures the CA extracts certain key fields of data from the certificate request and places these fields of data into an unsigned digital certificate.

[0040] A "Biometric Data Block" data structure of a specific format is created. Figures 4a and 4b depict possible formats for the data structure.

[0041] Figure 4a depicts a biometric data block into which the biometric data is placed, along with a digital signature of the biometric data and various fields of data which define parameters of the biometric data and signature.

[0042] Figure 4b depicts a biometric data block into which a reference to the location of biometric data is placed, along with a digital signature of the biometric data and various fields of data which define parameters of the biometric data and signature. The location of the biometric data may be specified in any manner of ways, including but not limited to a URL, a URN, or an XPath.

[0043] The biometric data block created in [0040] is embedded into the certificate extension portion of the unsigned digital certificate created in [0039].

[0044] The unsigned certificate is then signed by the CA in accordance with currently established cryptographic procedures, yielding a signed digital certificate.

[0045] The signed digital certificate is then conveyed to the original certificate requester through some means which are not in the scope of the invention.

[0046] 2. Certificate Validation.

[0047] Many distinct processes such as signing and identification on the Internet and in the real world ultimately depend on the validation of a digital certificate.

[0048] A block diagram of the established process of validating a digital certificate is presented in Figure 2a. In this process the certificate to be verified as well as the certificate of the signing CA are input into a "Verify Certificate" module which determines whether or not the certificate to be verified contains a valid signature applied by the CA. The module in effect produces a "Pass or Fail" result.

- [0049] Figure 2b represents a block diagram of the process of validating a digital signature and validating the biometric data bound to the certificate.
- [0050] In this process the certificate itself is validated using the conventional process presented in Figure 2a. In addition a parallel process of "Pass or Fail" validation of the bound biometric data is performed. If both of the validation processes pass, the certificate and biometric data to verify are deemed valid. If either process fails, the certificate shall be deemed invalid.
- [0051] Referring to figure 2b; the "Compare Biometrics" module takes two objects as input: 1) biometric data to verify, and 2) biometric data bound to the certificate.
- [0052] Referring to Figure 2b; the "Compare Biometrics" module compares biometric data in a manner which applies to the particular type of biometric data being compared. For example; fingerprint data may be compared using a algorithm which depends on statistical closeness of minutia sets, or a photograph may be compared to a live human with the help of a human authority standing at a security checkpoint.
- [0053] Referring to Figure 2b; the origin of the "Biometric Data to Verify" is not defined in the scope of the invention, but for illustrative purposes several representative origins and applications are presented below.
- [0054] Sample 1; a guard at an airport checkpoint manually verifies that the photograph derived from a certificate in a digital ID card matches the appearance of the person presenting the ID card.
- [0055] Sample 2; an ATM machine collects a fingerprint from a customer via a fingerprint reader device, and then uses a statistical minutia matching algorithm to determine if the fingerprint collected in real time matches the fingerprint derived from the certificate in the presented ATM card.
- [0056] Sample 3; an on-line access control device requires that the user present a smart card as well as speak a phrase into a microphone. The control device performs a comparison between the voiceprint derived from the smart card with the live voice print collected over the microphone.
- [0057] It will be noted that this description and the drawings are illustrative only and that

